UPPER BOUNDS ON CYCLOTOMIC NUMBERS

KOICHI BETSUMIYA, MITSUGU HIRASAKA, TAKAO KOMATSU, AND AKIHIRO MUNEMASA

Abstract. In this article, we give upper bounds for cyclotomic numbers of order e over a finite field with q elements, where e is a positive divisor of $q-1$. In particular, we show that under certain assumptions, cyclotomic numbers are at most $\lceil \frac{k}{2} \rceil$, and the cyclotomic number $(0,0)$ is at most $\lceil \frac{k}{2} \rceil - 1$, where $k = (q-1)/e$. These results are obtained by using a known formula for the determinant of a matrix whose entries are binomial coefficients.

1. Introduction

Let q be a power of a prime p. Let $GF(q)$ denote the Galois field with q elements and let α be a primitive element of $GF(q)$. According to [1, Section 2.2], for a positive divisor k of $q-1$ we define *cyclotomic numbers* of order $e = \frac{q-1}{k}$ as follows. For an integer a, let C_a denote the cyclotomic coset $\langle \alpha^e \rangle \alpha^a$. For integers a, b with $0 \le a, b < e$, the cyclotomic number (a, b) is defined as

$$(a, b) = |C_b \cap (C_a + 1)|.$$

These numbers appear as intersection numbers of a *cyclotomic scheme* whose non-diagonal relations are Cayley digraphs over $GF(q)$ with connection set C_a with $0 \le a \le e-1$ (see [2, p. 66]). For example, when $-1 \in C_0$, these Cayley digraphs are actually undirected, and $(0,0)$ is the number of common neighbors of two adjacent vertices. We remark that all of these Cayley digraphs are pairwise isomorphic, they are undirected if and only if k is even or $p = 2$, and each of them is a disjoint union of complete graphs if and only if $k+1$ is a power of p, in which case $(0,0) = k-1$.

Cyclotomic numbers have been studied since the beginning of the last century and they can be determined from the knowledge of Gauss sums. However, explicit evaluation of Gauss sums of large orders is difficult in general [1, pp. 98–99 and p. 152], so one cannot expect a

Date: October 4, 2011.

The second author thanks the support from the grant represented by the third author when the second author stayed at Hirosaki University from April 22-27 in 2011.

The third author is supported in part by the Grant-in-Aid for Scientific research (C) (No. 22540005), the Japan Society for the Promotion of Science.

general formula for cyclotomic numbers. Instead, we aim to establish upper bounds for cyclotomic numbers.

In 1972, Wilson [6] gave an inequality for higher cyclotomic numbers. This in particular gives upper and lower bounds for ordinary cyclotomic numbers. However, the inequality for ordinary cyclotomic numbers is a consequence of an exact evaluation of the variance of cyclotomic numbers [5]:

$$\sum_{a,b=0}^{e-1}((a,b)-\frac{q-2}{e^2})^2=(e-3)k+1+\frac{2k}{e}-\frac{1}{e^2}\le q-1. \tag{1}$$

For each fixed e, we see from (1) that the cyclotomic number (a,b) is close to $\frac{k}{e}$, that is,

$$(a,b)=\frac{k}{e}+O(\sqrt{k})\quad \text{as } k\to\infty. \tag{2}$$

However, when $e\ge k$, the formula does not seem to give any reasonable bound for (a,b) beyond the trivial bound $(a,b)\le k$. This is unavoidable since, when $k+1$ is a power of p, $(0,0)=k-1$ as we mentioned earlier. The purpose of this paper is to give upper bounds on cyclotomic numbers without assuming any relations among e and k, but instead, we need to assume that p is sufficiently large compared to k.

Theorem 1.1. *Let q be a power of an odd prime p and k a positive divisor of $q-1$. Then we have the following:*

(i) $(a,b)\le\lceil\frac{k}{2}\rceil$ *for all a,b with $0\le a,b<e$ if $p>\frac{3k}{2}-1$;*
(ii) $(a,a)\le\lceil\frac{k}{2}\rceil-1$ *for each a with $0\le a<e$ if k is odd and $p>\frac{3k}{2}$;*
(iii) $(0,0)\le\lceil\frac{k}{2}\rceil-1$ *if $p>\frac{3k}{2}$;*
(iv) $(0,0)=2$ *if p is sufficiently large and $6\mid k$;*
(v) $(0,0)=0$ *if p is sufficiently large and $6\nmid k$.*

Note that, if $2k+1$ is a power of p, then the upper bounds in Theorem 1.1(i),(ii) and (iii) are attained.

In the proof of Theorem 1.1(i),(ii) and (iii) we use a formula to expand the determinant of the matrix

$$\left(\binom{r+s}{r-i+j}\right)_{1\le i,j\le m} \tag{3}$$

given in [3]. In Section 3 we show that the cyclotomic number (a,b) is equal to $k-\operatorname{rank}C^{(a,b)}$, where $C^{(a,b)}$ is a certain matrix with entries in $GF(q)$ (see Lemma 3.1). Thus, giving a lower bound for the rank of $C^{(a,b)}$ results in an upper bound for the cyclotomic number (a,b). Since the matrix $C^{(a,b)}$ contains a submatrix which is the modulo p reduction of (3) for suitable r and s, we obtain a lower bound for the rank whenever the determinant does not vanish modulo p.

Though we reached [3] via [4], there is a typo in the formula (2) in [4], so that the simple expression (5) in [4] does not give the evaluation of the above determinant.

In Section 2 we will establish Wilson's formula (1). We include its proof as it has not been published. In Section 3 we will prepare some results to prove Theorem 1.1 in Section 4. In Section 5, we show that the inequality $(a, b) \le \lceil \frac{k}{2} \rceil$ holds under some assumptions different from the one in Theorem 1.1(i).

2. Wilson's formula

For the remainder of this article we use the same notation as in Section 1 and we shall write $GF(q)$ as F for short.

Lemma 2.1 (R. M. Wilson)**.** *Let*

$$X = \{(x, y) \in (F \setminus \{0, 1\})^2 \mid x \neq y,\ x \in yC_0,\ x - 1 \in (y - 1)C_0\},$$
$$Y = \{(u, v) \in (C_0 \setminus \{1\})^2 \mid u \neq v\}.$$

Then $f : X \to Y$ defined by

$$f(x, y) = \left(\frac{x}{y}, \frac{x - 1}{y - 1}\right)$$

is a bijection. In particular, $|X| = (k - 1)(k - 2)$.

Proof. If $(x, y) \in X$, then $\frac{x}{y}, \frac{x-1}{y-1} \in C_0 \setminus \{1\}$. Since $x \neq y$, we have $\frac{x}{y} \neq \frac{x-1}{y-1}$. Thus $f(x, y) \in Y$. The inverse mapping of f is given by

$$g(u, v) = \left(\frac{u(1 - v)}{u - v}, \frac{1 - v}{u - v}\right).$$

Since $|Y| = (k - 1)(k - 2)$, the second statement follows. □

Lemma 2.2. *We have the following:*

(i) $\sum_{a,b=0}^{e-1} (a, b) = q - 2$;

(ii) $\sum_{a,b=0}^{e-1} (a, b)^2 = (k - 1)(k - 2) + q - 2$.

Proof. (i)

$$\begin{aligned} \sum_{a,b=0}^{e-1} (a, b) &= \sum_{a,b=0}^{e-1} |(C_a + 1) \cap C_b| \\ &= \sum_{a=0}^{e-1} |(C_a + 1) \cap F^\times| \\ &= |(F^\times + 1) \cap F^\times| \\ &= |F \setminus \{0, 1\}| \\ &= q - 2. \end{aligned}$$

(ii)

$$\begin{aligned}
&\sum_{a,b=0}^{e-1}(a,b)^2-\sum_{a,b=0}^{e-1}(a,b)\\
&=\sum_{a,b=0}^{e-1}|\{(x,y)\in((C_a+1)\cap C_b)^2\mid x\neq y\}|\\
&=|\bigcup_{a,b=0}^{e-1}\{(x,y)\in((C_a+1)\cap C_b)^2\mid x\neq y\}|\\
&=|\{(x,y)\in(F\setminus\{0,1\})^2\mid x\neq y,\\
&\qquad \exists a\in\{0,1,\dots,e-1\},\ \{x-1,y-1\}\subset C_a,\\
&\qquad \exists b\in\{0,1,\dots,e-1\},\ \{x,y\}\subset C_b\}|\\
&=|\{(x,y)\in(F\setminus\{0,1\})^2\mid x\neq y,\ x\in yC_0,\ x-1\in(y-1)C_0\}|\\
&=|\{(u,v)\in C_0\setminus\{1\}\mid u\neq v\}|\\
&=(k-1)(k-2)
\end{aligned}$$

by Lemma 2.1. □

As mentioned in Section 1, Wilson showed the variance of cyclotomic numbers through [5].

Theorem 2.3 (Wilson)**.**

$$\sum_{a,b=0}^{e-1}((a,b)-\frac{q-2}{e^2})^2=(e-3)k+\frac{2k}{e}+1-\frac{1}{e^2}.$$

Proof. By Lemma 2.2, we have

$$\begin{aligned}
\sum_{a,b=0}^{e-1}((a,b)-\frac{q-2}{e^2})^2&=\sum_{a,b=0}^{e-1}(a,b)^2-\frac{2(q-2)}{e^2}\sum_{a,b=0}^{e-1}(a,b)+\frac{(q-2)^2}{e^2}\\
&=(k-1)(k-2)+q-2-\frac{2(q-2)^2}{e^2}+\frac{(q-2)^2}{e^2}\\
&=(e-3)k+\frac{2k}{e}+1-\frac{1}{e^2}.
\end{aligned}$$

□

Since

$$(e-3)k+\frac{2k}{e}+1-\frac{1}{e^2}\leq ek,$$

Theorem 2.3 implies

$$|(a,b)-\frac{q-2}{e^2}|<\sqrt{ek}, \tag{4}$$

Thus, for e fixed and $k \to \infty$,

$$\frac{1}{\sqrt{k}}|(a,b) - \frac{k}{e}| \leq \frac{1}{\sqrt{k}}(|(a,b) - \frac{q-2}{e^2}| + \frac{1}{e^2})$$
$$\leq \sqrt{e} + \frac{1}{e^2\sqrt{k}}$$

which is bounded. This implies (2).

Remark 2.1. By (4), we have

$$(a,b) < \frac{k}{e} + \sqrt{ek}.$$

If $\frac{k}{16} \geq e \geq 4$, then

$$(a,b) < \frac{k}{4} + \sqrt{\frac{k^2}{16}}$$
$$= \frac{k}{2}.$$

We shall show in the next section that a similar inequality holds without any assumption on e and k, if p is sufficiently large.

3. Cyclotomic numbers and determinants

Define a $k \times k$ matrix $C^{(a,b)}$ with entries in F for integers a, b by

$$\left(C^{(a,b)}\right)_{i,j} = \begin{cases} 1 + \alpha^{ak} - \alpha^{bk} & \text{if } i = j, \\ \binom{k}{j-i} & \text{if } i < j, \\ \alpha^{ak}\binom{k}{i-j} & \text{otherwise.} \end{cases}$$

Lemma 3.1.

$$(a,b) = k - \operatorname{rank} C^{(a,b)} = \deg(\gcd((X+1)^k - \alpha^{bk}, X^k - \alpha^{ak})).$$

Proof. For simplicity, write $\beta = \alpha^{ak}$ and $\gamma = 1 + \beta - \alpha^{bk}$. Let T denote the following $k \times k$ matrix:

$$T = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \beta & & & \end{pmatrix}.$$

Then T has the characteristic polynomial $\psi(X) = X^k - \beta$ which has k distinct roots in F. Define another polynomial $\phi(X)$ by

$$\phi(X) = (X+1)^k - \alpha^{bk}.$$

Then

$$C^{(a,b)} = \gamma I + \sum_{i=1}^{k-1} \binom{k}{i} T^i$$

$$
\begin{aligned}
&= (1+\beta-\alpha^{bk})I + \sum_{i=1}^{k-1}\binom{k}{i}T^i \\
&= I + T^k - \alpha^{bk}I + \sum_{i=1}^{k-1}\binom{k}{i}T^i \\
&= (T+I)^k - \alpha^{bk}I \\
&= \phi(T).
\end{aligned}
$$

The multiplicity of 0 as an eigenvalue of $C^{(a,b)}$ is the number of eigenvalues θ of T with $\phi(\theta)=0$. Thus

$$
\begin{aligned}
k - \operatorname{rank} C^{(a,b)} &= |\{\theta \mid \theta \text{ is an eigenvalue of } T,\ \phi(\theta)=0\}| \\
&= |\{x \in F \mid \psi(x)=\phi(x)=0\}| \\
&= |\{x \in F \mid x^k=\alpha^{ak},\ (x+1)^k=\alpha^{bk}\}| \\
&= |\{x \in F \mid x \in \langle\alpha^e\rangle\alpha^a,\ x+1 \in \langle\alpha^e\rangle\alpha^b\}| \\
&= |(C_a+1)\cap C_b| \\
&= (a,b).
\end{aligned}
$$

Since (a,b) is the number of common roots in F of $\phi(X)$ and $\psi(X)$, the second equality holds. $\square$

Let $m=\left\lfloor \frac{k}{2}\right\rfloor$. The upper right $m\times m$ submatrix of $C^{(a,b)}$ is

$$
\begin{pmatrix}
\binom{k}{m} & \binom{k}{m+1} & \cdots & \binom{k}{2m-1} \\
\vdots & \vdots & & \vdots \\
\binom{k}{1} & \binom{k}{2} & \cdots & \binom{k}{m}
\end{pmatrix} \quad \text{if } k=2m, \tag{5}
$$

$$
\begin{pmatrix}
\binom{k}{m+1} & \binom{k}{m+2} & \cdots & \binom{k}{2m} \\
\vdots & \vdots & & \vdots \\
\binom{k}{2} & \binom{k}{3} & \cdots & \binom{k}{m+1}
\end{pmatrix} \quad \text{if } k=2m+1, \tag{6}
$$

whose determinants can be calculated.

Lemma 3.2 ([3, Section 2.2])**.** *Let r,s,m be integers with $r,s,m\geq 0$. Then*

$$
\det\left(\binom{r+s}{r-i+j}\right)_{1\leq i,j\leq m} = \prod_{i=0}^{m-1}\frac{i!(r+s+i)!}{(r+i)!(s+i)!}.
$$

By Lemma 3.2, the matrices (5) and (6) have determinants

$$
\prod_{i=0}^{m-1}\frac{i!(k+i)!}{(m+i)!(k-m+i)!} \quad \text{if } k=2m, \tag{7}
$$

$$
\prod_{i=0}^{m-1}\frac{i!(k+i)!}{(m+1+i)!(k-m-1+i)!} \quad \text{if } k=2m+1, \tag{8}
$$

respectively.

Similarly, the matrix

$$\begin{pmatrix} \binom{k}{m} & \binom{k}{m+1} & \cdots & \binom{k}{2m-1} & \binom{k}{2m} \\ \vdots & \vdots & & \vdots & \\ \binom{k}{1} & \binom{k}{2} & \cdots & \binom{k}{m} & \binom{k}{m+1} \\ \binom{k}{0} & \binom{k}{1} & \cdots & \binom{k}{m-1} & \binom{k}{m} \end{pmatrix} \tag{9}$$

has determinant

$$\prod_{i=0}^{m} \frac{i!(k+i)!}{(m+i)!(k-m+i)!}. \tag{10}$$

4. Bounds

Proposition 4.1. *If $p > \frac{3k}{2} - 1$, then $(a,b) \leq \lceil \frac{k}{2} \rceil$ for all a, b with $0 \leq a, b < e$.*

Proof. Let $m = \lfloor \frac{k}{2} \rfloor$. Since $p > k + m - 1$, the determinant (7) (resp. (8)) is nonzero modulo p when $k = 2m$ (resp. $k = 2m+1$), hence $\operatorname{rank} C^{(a,b)} \geq \lfloor \frac{k}{2} \rfloor$. The result then follows from Lemma 3.1. □

The result of Proposition 4.1 can be improved for $\lambda = (0,0)$.

Proposition 4.2. *Suppose $p > \frac{3k}{2}$. Then we have the following:*

(i) *If k is odd, then $(a,a) \leq \lceil \frac{k}{2} \rceil - 1$ for all a with $0 \leq a < e$;*
(ii) $(0,0) \leq \lceil \frac{k}{2} \rceil - 1$.

Proof. If $k = 2m+1$, then the upper right $(m+1) \times (m+1)$ submatrix of $C^{(a,a)}$ is given by (9). If $k = 2m$, then the $(m+1) \times (m+1)$ submatrix of $C^{(0,0)}$ consisting of the first $m+1$ rows, the upper right m columns and the first column is also given by (9). Since $p > \frac{3k}{2}$, the determinant (10) is nonzero modulo p, hence $\operatorname{rank} C^{(a,a)} \geq \frac{k+1}{2}$ if k is odd, and $\operatorname{rank} C^{(0,0)} \geq \frac{k}{2} + 1$ if k is even. The result then follows from Lemma 3.1. □

Proposition 4.3. *Let λ denote the cyclotomic number $(0,0)$. If p is sufficiently large, then $\lambda = 2$ or $\lambda = 0$, according as $k \equiv 0 \pmod 6$ or not.*

Proof. Since the matrix $C^{(0,0)}$ does not involve β or γ as entries, we may regard it as a matrix over $\mathbb{Z}$. The eigenvalues of $C^{(0,0)}$ are

$$(\zeta^j + 1)^k - 1 \quad (j = 0, 1, \ldots, k-1)$$

where $\zeta = \exp \frac{2\pi i}{k}$. This is zero only if $k \equiv 0 \pmod 6$, and $\zeta^j = \exp \frac{2\pi i}{3}$ or $\exp \frac{4\pi i}{3}$. If $k \not\equiv 0 \pmod 6$, all the eigenvalues of $C^{(0,0)}$ are nonzero, hence $C^{(0,0)}$ is invertible in characteristic 0. This implies that $\det C^{(0,0)}$ is a nonzero integer. If $p > |\det C^{(0,0)}|$, then $C^{(0,0)}$ is invertible in characteristic p, hence $\lambda = 0$ by Lemma 3.1.

If $k \equiv 0 \pmod 6$, then the multiplicity of 0 as an eigenvalue of $C^{(0,0)}$ is 2. This implies that $C^{(0,0)}$ contains a $(k-2) \times (k-2)$ minor whose determinant is nonzero in characteristic 0. Thus, if p is sufficiently large, $C^{(0,0)}$ has rank $k-2$, hence $\lambda = 2$ by Lemma 3.1. $\square$

When $k \not\equiv 0 \pmod 6$, there are only finitely many primes p which divide $\det C^{(0,0)}$. This means that the set of characteristics p for which $\lambda > 0$ holds is finite. However, as we do not know any formula for $\det C^{(0,0)}$, we do not know the set of characteristics for which $\lambda > 0$ holds.

Proof of Theorem 1.1. All the statements are direct consequences of the above propositions. $\square$

5. Additional results

We set $\beta = \alpha^{ak}$, $\gamma = 1 + \beta - \alpha^{bk}$, and define $\phi, \psi \in F[X]$ by

$$\phi(X) = (X+1)^k - \alpha^{bk},\ \psi(X) = X^k - \beta,$$

as in the proof of Lemma 3.1. Define $\phi_0 \in F[X]$ by

$$\begin{aligned} \phi_0(X) &= \phi(X) - \psi(X) \\ &= \gamma + \sum_{i=1}^{k-1} \binom{k}{i} X^i. \end{aligned}$$

Let J denote the ideal of $F[X]$ generated by ϕ_0 and ψ. Then it follows from Lemma 3.1 that

$$(a,b) = \min\{\deg \rho \mid 0 \neq \rho \in J\}. \tag{11}$$

Proposition 5.1. *If $\frac{3k}{4} \leq p < k$, then $(a,b) \leq \left\lfloor \frac{k}{2} \right\rfloor$ for all a, b with $0 \leq a, b < e$.*

Proof. We claim that, for each i with $k - p + 1 \leq i \leq p - 1$,

$$\binom{k}{i} \equiv 0 \pmod p.$$

This follows since $k(k-1)\cdots(k-i+1) \equiv 0 \pmod p$ while $i! \not\equiv 0 \pmod p$.

Note that

$$\begin{aligned} &X^{k-p}\phi_0(X) - \sum_{i=p}^{k-1} \binom{k}{i} \psi(X) X^{i-p} \\ &= \gamma X^{k-p} + \sum_{i=1}^{k-p} \binom{k}{i} X^{i+k-p} + \beta \sum_{i=p}^{k-1} \binom{k}{i} X^{i-p} \\ &\quad + \sum_{i=k-p+1}^{p-1} \binom{k}{i} X^{i+k-p}, \end{aligned}$$

and the last summand is zero by the claim. Since

$$\binom{k}{k-p} = \binom{k}{p} \not\equiv 0 \pmod{p}$$

by the assumption, J contains a nonzero polynomial of degree $2k-2p$. It follows from (11) and the assumption on p that

$$(a,b) \leq 2k - 2p \leq 2k - 2 \cdot \frac{3k}{4} = \frac{k}{2}.$$

This implies that $(a,b) \leq \left\lfloor \frac{k}{2} \right\rfloor$. ☐

Proposition 5.2. *If $k+1 < p^t < \frac{3k}{2}$ for some positive integer t, then $(a,b) \leq \left\lfloor \frac{k}{2} \right\rfloor$ and $(a,a) \leq \left\lfloor \frac{k}{2} \right\rfloor - 1$ for all a, b with $0 \leq a, b < e$.*

Proof. We set $m = \left\lfloor \frac{k}{2} \right\rfloor$. For each positive integer i with $i \leq k-1$, we define $\phi_i \in J$ by

$$\phi_i(X) = X^i \phi_0(X) - \psi(X) \sum_{j=0}^{i-1} \binom{k}{i-j} X^j.$$

Then

$$\phi_i(X) = \gamma X^i + \beta \sum_{j=0}^{i-1} \binom{k}{i-j} X^j + \sum_{j=i+1}^{k-1} \binom{k}{j-i} X^j,$$

and hence $\deg(\phi_i) \leq k-1$. Let

$$f(X) = \sum_{i=0}^{m} \binom{p^t - k}{m-i} \phi_i(X) = \sum_{l=0}^{k-1} a_l X^l.$$

For $0 \leq i \leq l < k$, the coefficient of X^l in

$$\psi(X) \sum_{j=0}^{i-1} \binom{k}{i-j} X^j$$

is zero. This implies that $\phi_i(X)$ and $X^i \phi_0(X)$ have the same coefficient at degree l. Thus, for $m < l \leq k-1$,

$$\begin{aligned} a_l &= \sum_{i=0}^{m} \binom{p^t - k}{m-i} \binom{k}{l-i} \\ &= \binom{p^t}{m+k-l} \\ &= 0, \end{aligned}$$

and

$$a_m = \sum_{i=0}^{m-1} \binom{p^t - k}{m-i} \binom{k}{m-i} + \gamma$$

$$
\begin{aligned}
&= \binom{p^t}{k} + \gamma - 1 \\
&= \gamma - 1.
\end{aligned}
$$

We claim that $a_{m-1} = \beta k$ if $\gamma = 1$. Since the coefficient of X^{m-1} in

$$
\psi(X) \sum_{j=0}^{m-1} \binom{k}{m-j} X^j
$$

is $-\beta k$, we have

$$
\begin{aligned}
a_{m-1} &= \sum_{i=0}^{m-1} \binom{p^t - k}{m-i} \binom{k}{m-1-i} + \beta k \\
&= \sum_{j=0}^{m-1} \binom{p^t - k}{j+1} \binom{k}{j} + \beta k \\
&= \sum_{j=0}^{k} \binom{p^t - k}{j+1} \binom{k}{k-j} + \beta k \qquad\qquad (\text{since } p^t - k \leq m) \\
&= \binom{p^t}{k+1} + \beta k \\
&= \beta k.
\end{aligned}
$$

Therefore, $\deg(f) = m$ if $\gamma \neq 1$, and $\deg(f) = m - 1$ if $\gamma = 1$ or equivalently $a = b$. Since $f \in J$, it follows from (11) that $(a, b) \leq m$ and $(a, a) \leq m - 1$. $\square$

Acknowledgements. The authors would like to thank Richard M. Wilson for suggesting the use of his formula for the variance of cyclotomic numbers.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, John Wiley & Sons, Inc., New York, 1998.

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-Regular Graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 18. Springer-Verlag, Berlin, 1989.

[3] C. Krattenthaler, Advanced Determinant Calculus, Sém. Lothar. Combin. 42 ("The Andrews Festschrift"), 1999, Article B42q, 67pp.

[4] R. Pemantle and H. S. Wilf, Counting nondecreasing integer sequences that lie below a barrier, Electron. J. Combin. 16 (2009), no. 1, Research Paper 60, 7 pp.

[5] R.M. Wilson, private communication, 2011.

[6] R.M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory 4 (1972), 17-47.

E-mail address: `betsumi@cc.hirosaki-u.ac.jp`

Graduate School of Science and Technology, Hirosaki University, Hirosaki 036-8561, Japan

E-mail address: hirasaka@pusan.ac.kr

Department of Mathematics, Pusan National University, Jang-jeon dong, Busan 609-735, Korea

E-mail address: komatsu@cc.hirosaki-u.ac.jp

Graduate School of Science and Technology, Hirosaki University, Hirosaki 036-8561, Japan

E-mail address: munemasa@math.is.tohoku.ac.jp

Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan